



98-367^{Q&As}

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/98-367.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

The default password length for a Windows Server domain controller is:

- A. 0
- B. 5
- C. 7
- D. 14

Correct Answer: C

QUESTION 2

Which of the following is method that can be used to identify Internet software in Software Restriction Policies?

- A. Restriction rule
- B. Identification rule
- C. Internet rule
- D. Zone rule

Correct Answer: D

Zone rule is method that can be used to identify Internet software in Software Restriction Policies. Answer: C, B, and A are incorrect. These are invalid Answer: .

QUESTION 3

What are the main classes of biometric characteristics? Each correct answer represents a complete solution. Choose two.

- A. Psychological
- B. Behavioral
- C. Fundamental
- D. Physiological

Correct Answer: BD

Answer: D and B

A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits. Biometrics is used as a form of identity access management and access control. It is also used to identify individuals



in groups that are under surveillance.

Biometric characteristics can be divided into two main classes:

1. Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely replaced the retina and odor/scent.

2. Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

Answer: A and C are incorrect. These are not the classes of biometric characteristics.

QUESTION 4

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

Hot Area:

Answer Area

	Yes	No
To protect users from untrusted browser pop-ups, you may set a default browser configuration that blocks all pop-ups and automated downloads.	<input type="checkbox"/>	<input type="checkbox"/>
Online pop-ups and dialog boxes can display a realistic operating system or application error messages.	<input type="checkbox"/>	<input type="checkbox"/>
Protecting users from untrusted pop-up applications is mostly a function of awareness.	<input type="checkbox"/>	<input type="checkbox"/>

Correct Answer:

**Answer Area**

Yes

No

To protect users from untrusted browser pop-ups, you may set a default browser configuration that blocks all pop-ups and automated downloads.

☐☒

Online pop-ups and dialog boxes can display a realistic operating system or application error messages.

☒☐

Protecting users from untrusted pop-up applications is mostly a function of awareness.

☒☐**QUESTION 5**

Which of the following is used to protect all files stored on the drive on which Windows is installed?

- A. SocketShield
- B. Firewall
- C. BitLocker
- D. Hardware keylogger

Correct Answer: C

BitLocker is used to protect all files stored on the drive on which Windows is installed. It encrypts the entire system drive and helps block hackers from accessing the system files they rely on to discover user passwords. BitLocker also

prevents hackers from accessing the hard disk by removing it from a computer, and installing it on a different computer. BitLocker does not work for USB Flash Drives. Answer:

A is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various types of keyloggers. SocketShield provides protection at the following two levels:

1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in these domains are simply blocked.

2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.

Answer: B is incorrect. A firewall is a system that helps in preventing access to a system from unauthorized internet or network users. A firewall can be hardware as well as software. A firewall is implemented on systems that are connected to



the internet and are vulnerable to hackers, viruses, worms, and other harmful intrusions. Answer: D is incorrect. Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including

sensitive passwords. They can be implemented via BIOS-level firmware, or alternatively, via a device plugged inline between a computer keyboard and a computer. They log all keyboard activities to their internal memory.

QUESTION 6

How does the sender policy framework (SPF) aim to reduce spoofed email?

- A. It provides a list of IP address ranges for particular domains so senders can be verified.
- B. It includes an XML policy file with each email that confirms the validity of the message.
- C. It lists servers that may legitimately forward mail for a particular domain.
- D. It provides an encryption key so that authenticity of an email message can be validated

Correct Answer: A

QUESTION 7

Which of the following is a collection or list of user accounts or computer accounts?

- A. Group
- B. Active Directory
- C. Domain
- D. Public folder

Correct Answer: A

A group is a collection or list of user accounts or computer accounts. Groups can be used to simplify administration, especially when assigning rights and permissions. Answer: B is incorrect. Active Directory is a centralized and standardized system that is available with the Windows Server 2008 platform. Active Directory stores information in a central database and allows users to have a single user account called "domain user account" for the network. Active Directory helps to automate network management of user data, security, and distributed resources, thereby enabling interoperability with other directories. Active Directory is Microsoft's trademarked directory service, an integral part of the Windows architecture. This directory is especially designed for distributed networking environments. Answer: C is incorrect. In the Windows environment, a domain is a set of network resources that are part of a network and share a common directory database. A domain is administered as a unit with common rules and procedures. Each domain has a unique name. Users just have to log on to a domain to access the network resources within it. Answer: D is incorrect. A public folder is a storage area on public information store. It is used to collect, organize, and share information among users in an organization. It provides a permanent storage place. Moreover, it can be used to post information on an electronic bulletin board and store sharable items, i.e., calendars and contacts, etc. A public folder can be created and configured in an Exchange organization by administrators and other users who have sufficient access permissions.

QUESTION 8



What are three major attack vectors that a social engineering hacker may use? (Choose three.)

- A. Telephone
- B. Reverse social engineering
- C. Waste management
- D. Honey pot systems
- E. Firewall interface

Correct Answer: ABC

QUESTION 9

This question requires that you evaluate the underlined text to determine if it is correct.

To determine which action, if any, to take on an inbound message, anti-spam and antivirus recipient filtering inspects the IP address of the remote server that is trying to send messages.

Instructions: Review the underlined text. If it makes the statement correct, select "No change is needed." If the statement is incorrect, select the answer choice that makes the statement correct.

- A. connection
- B. sender
- C. content
- D. No change is needed

Correct Answer: A

References: <https://docs.microsoft.com/en-us/office365/SecurityCompliance/configure-the-connection-filter-policy>

QUESTION 10

Creating MD5 hash for files is an example of ensuring what?

- A. Confidentiality
- B. Availability
- C. Least privilege
- D. Integrity

Correct Answer: D

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

**QUESTION 11**

Which of the following are the main features of a key logger? Each correct answer represents a complete solution. Choose all that apply.

- A. It can be delivered via FTP or e-mail.
- B. It can record all keystrokes.
- C. It can capture all screenshots.
- D. It can detect viruses on the computer.

Correct Answer: ABC

Answer: A, B, and C

A keylogger is a software tool that traces all or specific activities of a user on a computer. Once a keylogger is installed on a victim's computer, it can be used for recording all keystrokes on the victim's computer in a predefined log file. An

attacker can configure a log file in such a manner that it can be sent automatically to a predefined e-mail address. Some of the main features of a keylogger are as follows:

It can record all keystrokes.

It can capture all screenshots.

It can record all instant messenger conversations. It can be remotely installed.

It can be delivered via FTP or e-mail.

Answer: D is incorrect. It cannot detect viruses.

QUESTION 12

Which of the following are the major components of the IPsec protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. Encapsulating Security Payload (ESP)
- B. Authentication Header (AH)
- C. Internet Encryption Key (IEK)
- D. Internet Key Exchange (IKE)

Correct Answer: ABD

Answer: B, A, and D

The IPsec protocol has three major components:



1. Authentication Header (AH)
2. Encapsulating Security Payload (ESP)
3. Internet Key Exchange (IKE)

Answer: C is incorrect. There is no such component of the IPSec protocol as Internet Encryption Key.

QUESTION 13

Mark works as a Network Administrator for BlueWell Inc. The company has a Windows-based network. Mark has retained his services to perform a security assessment of the company's network that has various servers exposed to the Internet. So, it may be vulnerable to an attack. Mark is using a single perimeter firewall, but he does not know if that is enough. He wants to review the situation and make some reliable recommendations so that he can protect the data over company's network. Which of the following will Mark do to accomplish the task?

- A. Outsource the related services.
- B. Encrypt the data and then start transmission.
- C. Locate the Internet-exposed servers and devices in an internal network.
- D. Create a perimeter network to isolate the servers from the internal network.

Correct Answer: D

In the above scenario, Mark will create a perimeter network to isolate the servers from the internal network because Internet-exposed servers and devices should not be located in an internal network. They have to be segmented or isolated into a protected part of the network.

QUESTION 14

A process by which DNS zone data is obtained by an attacker is referred to as:

- A. spoofing
- B. footprinting
- C. phishing
- D. Denial of Service

Correct Answer: B

QUESTION 15

You are an intern and are working remotely.

You need a solution that meets the following requirements: Allows you to access data on the company network securely
Gives you the same privileges and access as if you were in the office



What are two connection methods you could use? (Choose two.)

- A. Forward Proxy
- B. Virtual Private Network (VPN)
- C. Remote Access Service (RAS)
- D. Roaming Profiles

Correct Answer: BD

[Latest 98-367 Dumps](#)

[98-367 PDF Dumps](#)

[98-367 Practice Test](#)